UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,861	10/06/2003	Craig Ogg	61135/P023US/10303235	3194

29053 7590 05/25/2010

FULBRIGHT & JAWORSKI L.L.P
2200 ROSS AVENUE
SUITE 2800
DALLAS, TX 75201-2784

EXAMINER	
ROBINSON BOYCE, AKIBA K	
ART UNIT	**PAPER NUMBER**
3628	

MAIL DATE	DELIVERY MODE
05/25/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/679,861	OGG, CRAIG	
	Examiner	Art Unit	
	AKIBA K. ROBINSON BOYCE	3628	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 April 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-7,9-13,15-22 and 29-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-7,9-13,15-22 and 29-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/12/10 has been entered.

Status of Claims

2. Due to communications filed 4/12/10, the following is a non-final office action. Claims 2-7, 9-13, 15-18, 21, 29-38 have been amended. Claims 1, 8, 14, 23-28 are cancelled. Claims 39-42 are new. Claims 2-7, 9-13, 15-22 and 29-42 are pending in this application and have been examined on the merits. The previous rejection has been modified to reflect claim amendments. Claims 2-7, 9-13, 15-22 and 29-42 are rejected as follows.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 6 and 7 recite the limitation " the authorization database". There is insufficient antecedent basis for this limitation in the claim.

Claim Objections

5. Claim 42 is objected to because of the following informalities: This claim depends on claim 43 which does not exist. Examiner interprets claim 42 as being dependent on claim 41. Appropriate correction is required.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 39, 2-5, 9-11, 15-18, 34, 35, 38 are rejected under 35 U.S.C. 102(b) as being anticipated by Lee et al, (US 5,742,683).

As per claim 39, Lee et al discloses:

at least one postage usage meter parameter, wherein said meter parameter limits all users' of said plurality of users ability to evidence postage using the meter, (non-operational state, col. 3, lines 16-21, The idle time of the vault is continuously monitored so that the vault can be placed in a non-operational state if the continuous idle time exceeds an idle time limit. The method of the present invention provides security that prevents tampering and false evidence of postage payment and provides the ability to do batch processing of digital tokens);

at least one postage usage user parameter corresponding to a particular user of said plurality of users, wherein said user parameter limits said particular user's ability to evidence postage using the meter, and wherein each respective particular user of said plurality of users corresponds to a respective user parameter, (col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open metering system in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password. Examples of such user functions/features that are customized to a user password are: vault refill, network meter access, maximum postage amount, destination address limitations, diagnostic and inspection report access, and departmental accounting reports via a local open metering system or a networked open metering system); and

wherein said postage evidencing meter is operable to limit said particular user's ability to evidence postage using said meter in accordance with said at least one meter parameter and said at least one user parameter, (col. 7, lines 27-46, shows PC-based postage meter 10 can function as a multiple-user device in which multiple users can have different access privilege levels to the meter features and functions. In the preferred embodiment, a setup routine will allow the primary or administrative user of PC-based postage meter 10 to customize individual user passwords for access to the

different meter features and functions, and shows an example where performance of the meter refill function may be restricted to the owner of the meter or a user assigned as an administrative user. This restriction is a common security feature since refilling the meter is spending money. The meter owner may also limit the number of users that are authorized to perform other functions of the meter, for example, changing any of the meter parameters, such as postage limit. Such users may share a single password to perform certain level(s) of functions or may each be given an individual password for added security).

As per claim 2, Lee et al discloses:

Wherein the user parameter comprises a maximum postage amount that the particular user is allowed to use on the meter to evidence postage (Col. 2, line 61, maximum postage amount).

As per claim 4, Lee et al discloses:

wherein a first user parameter of said at least one user parameter comprises a maximum postage amount that said particular user of said plurality of users is allowed to use on the meter to evidence postage and wherein a second user parameter of said at least one user parameter comprises a period of time during which the particular user of said plurality of users is allowed to use the meter to evidence postage, (col. 2, lines 41-45, The method provides password controlled access to the PC-based metering system wherein the use associated with each user password can be customized for

restricted access to various functions of the metering system, and col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open metering system in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password. Examples of such user functions/features that are customized to a user password are: vault refill, network meter access, maximum postage amount,)

As per claim 5, Lee et al discloses:
a user interface, (col. 4, line 26, user interface)

a printer, (col. 4, lines 34-35,non-secured digital printer); and

a security module, (col. 5, lines 14-20, encryption module).

As per claim 9, Lee et al discloses:
Wherein at least one user parameter comprises s a maximum postage amount that the particular user is allowed to use on the meter to evidence postage (Col. 2, line 61, maximum postage amount).

As per claim 10, Lee et al discloses:
wherein the at least one user parameter includes a period of time during which the particular user is allowed to use the meter to evidence postage (Col. 2, line 61, inherent

with network meter access since the user must access the meter for a certain amount of time).

As per claim 11, Lee et al discloses:

wherein the a first user parameter of the at least one user parameter includes a maximum postage amount that selected the particular user of said plurality of users is allowed to use on the meter to evidence postage and wherein a second user parameter of the at least one user parameter include a period of time during which the particular user of said plurality of users is allowed to use the meter to evidence postage, (col. 2, lines 41-45, The method provides password controlled access to the PC-based metering system wherein the use associated with each user password can be customized for restricted access to various functions of the metering system, and col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open metering system in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password. Examples of such user functions/features that are customized to a user password are: vault refill, network meter access, maximum postage amount,)

As per claim 15, Lee et al discloses:

at least two postage evidencing meters, each meter having a processor and a communication module for providing a communication link between the at least two meters wherein each of said at least two meters store at least one postage usage meter parameter that defines meter usage limits for the respective meter storing the meter parameter, and wherein at least one postage evidencing meter of said at least two postage evidencing meters stores at least one postage usage user parameter for each user of a plurality of users, wherein each of said user parameters define meter usage limits for a particular user associated with the user parameter, (Figs 2 and 8, col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open metering system in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password. Examples of such user functions/features that are customized to a user password are: vault refill, network meter access, maximum postage amount, destination address limitations, diagnostic and inspection report access, and departmental accounting reports via a local open metering system or a networked open metering system) ;

wherein at least one user parameter for at least one said particular user of said plurality of users is exchanged between said meters via the communication link, (col. 7,

lines 41-43, users may share a single password to perform certain level(s) of functions or may each be given an individual password for added security, also see Fig 8); and

wherein the processor of the meter receiving said user parameter controls an ability of the particular user associated with user parameter to evidence postage using the receiving meter in accordance with the received user parameter and at least one of the meter parameters stored by the receiving meter,(col. 3, lines 5-20, Each of the modes is assigned with a user password that is required to operate the vault in the respective mode. Each user of the vault is provided with one or more passwords corresponding to the access level assigned to the user. When the vault becomes operational a normal mode password is required to place the vault in normal mode. Once operational, whenever a command is received by the vault for a function corresponding to the manufacturing mode, the service mode or the privileged mode the command must be accompanied by a respective user password. The idle time of the vault is continuously monitored so that the vault can be placed in a non-operational state if the continuous idle time exceeds an idle time limit. The method of the present invention provides security that prevents tampering and false evidence of postage payment and provides the ability to do batch processing of digital tokens).

As per claim 16, Lee et al discloses:

Wherein the at least one user parameter comprises a maximum postage amount that the selected user is allowed to use on the meter to evidence postage (Col. 2, line

61, maximum postage amount).

As per claim 17, Lee et al discloses:

Wherein the at least one user parameter comprises a maximum amount of postage that can be evidenced by the selected user during a selected period of time (Col. 2, line 61, inherent with network meter access since the user must access the meter for a certain amount of time).

As per claim 18, Lee et al discloses:

wherein the a first user parameter said at least one user parameter comprises a maximum postage amount that the particular user is allowed to use on the meter to evidence postage and wherein a second user parameter of said at least one user parameter comprises a period of time during which the selected particular user is allowed to use the meter to evidence postage, (col. 2, lines 41-45, The method provides password controlled access to the PC-based metering system wherein the use associated with each user password can be customized for restricted access to various functions of the metering system, and col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open metering system in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what

functions/features were customized as being accessible for the entered user password. Examples of such user functions/features that are customized to a user password are: vault refill, network meter access, maximum postage amount,)

As per claim 34, Lee et al discloses:

wherein the at least one user parameter comprises at least one of time and amount (Col. 2, line 61, maximum postage amount).

As per claim 35, Lee et al discloses:

wherein the particular user is associated with at least two user parameters (col. 2, lines 41-45, The method provides password controlled access to the PC-based metering system wherein the use associated with each user password can be customized for restricted access to various functions of the metering system, and col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open metering system in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password. Examples of such user functions/features that are customized to a user password are: vault refill, network meter access, maximum postage amount,).

. As per claim 38, Lee et al discloses:

wherein the at least a particular user is associated with at least two user parameters (col. 2, lines 41-45, The method provides password controlled access to the PC-based metering system wherein the use associated with each user password can be customized for restricted access to various functions of the metering system, and col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open metering system in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password. Examples of such user functions/features that are customized to a user password are: vault refill, network meter access, maximum postage amount,)

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 3, 6, 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al, (US 5,742,683).

As per claim 3, Lee et al discloses:

Wherein the user parameter comprises a period of time during which the particular user of said plurality of users is allowed to use the meter to evidence postage, (obvious with network meter access since the user must access the meter for a certain amount of time).

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention for the user parameter comprises a period of time during which the particular user of said plurality of users is allowed to use the meter to evidence postage with the motivation of showing a representation of the period of access.

10.

As per claim 6, Lee et al discloses:

wherein the authorization database is stored on a removable storage device, (Claim 6 of Lee et al shows wherein said vault means comprises a portable vault card that is removably coupled to said PC, said PC including means for removably coupling said vault card to said PC and col. 7, line 64-col. 8, line 2, At step 120, a check is made to determine if the entered user password is authorized to perform such request. If not, the vault returns to an idle status at step 104, preferably sending a message to the user that the request is not authorized. If authorized, at steps 122-128, the requested function is performed, thereby suggesting some type of database means since in order to compare and confirm passwords the correct passwords must be stored).

It would have been obvious to one of ordinary skill in the art to provide an authorization database with the motivation of providing means for storage of passwords.

As per claim 7, Lee et al discloses:

Wherein the authorization database is coupled to the meter via a communication link to a remote postage information system (col. 3, lines 62-65, User interface module 42 also provides application programs the capability to initiate remote refills and to perform administrative functions, and col. 7, line 64-col. 8, line 2, At step 120, a check is made to determine if the entered user password is authorized to perform such request. If not, the vault returns to an idle status at step 104, preferably sending a message to the user that the request is not authorized. If authorized, at steps 122-128, the requested function is performed, thereby suggesting some type of database means since in order to compare and confirm passwords the correct passwords must be stored).

It would have been obvious to one of ordinary skill in the art to provide an authorization database with the motivation of providing means for storage of passwords.

11. Claims 21, 29-33, 36, 37, 40-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al and further in view of Liechti et al (US 5,715,164)

As per claim 21, Lee et al discloses:

wherein said communication link is used to transfer securely between the at least two meters using cryptographic techniques, (col. 1, line 57-col. 2, line 6, shows that typical information which may be encrypted as part of a digital token includes origination postal code, vendor identification, data identifying the PED, piece count, postage amount, date, and, for an open system, destination postal code. These items of information, collectively referred to as Postal Data, when encrypted with a secret key and printed on a mall piece provide a very high level of security which enables the detection of any attempted modification of a postal revenue block or a destination postal code. A postal revenue block is an image printed on a mall piece that includes the digital token used to provide evidence of postage payment. The Postal Data may be printed both in encrypted and unencrypted form in the postal revenue block. Postal Data serves as an input to a Digital Token Transformation which is a cryptographic transformation computation that utilizes a secret key to produce digital tokens. Results of the Digital Token Transformation, i.e., digital tokens, are available only after completion of the Accounting Process, and col. 4, lines 38-47, Electronic vault 20, which is housed in a removable card, such as PCMCIA card 30, is a secure encryption device for postage funds management, digital token generation and traditional accounting functions. PC meter system 10 may also include an optional modem 29 which is located preferably in PC 12. Modem 29 may be used for communicating with a Postal Service or a postal authenticating vendor for recharging funds (debit or credit). In an alternate embodiment the modem may be located in PCMCIA card 30.).

Lee et al does not specifically disclose wherein said at least one meter postage usage parameter is a meter balance, however, Liechti et al in col. 10, lines 18-45 shows meter balance is incorporated into the meter parameter. It would have been obvious to combine the teachings of Lee et al and Liechti et al to disclose wherein said at least one meter postage usage parameter is a meter balance with the motivation of showing that meter balance can be incorporated into evidencing of postage.

As per claim 29, Lee et al discloses:

separately storing at least one postage usage user parameter for each user of a plurality of users of a postage meter in a postage usage database, wherein said parameters establish separate postage evidencing limits for each user of said plurality of users, (col. 8, lines 41-46, users may share a single password to perform certain level(s) of functions or may each be given an individual password for added security. PC-based postage meter 10 keeps a log, which is stored on hard drive 24, of all transactions and logins for further security, w/ lines 38-47, shows that the Electronic vault 20, is housed in a removable card, such as PCMCIA card 30, thereby making it obvious to have a database that stores a postage usage user parameter for each user of a plurality of users) ***;***

storing at least one postage usage meter parameter, wherein said meter parameter establishes postage evidencing limits for all users of said postage meter, (non-operational state, col. 3, lines 16-21, The idle time of the vault is continuously monitored

so that the vault can be placed in a non-operational state if the continuous idle time exceeds an idle time limit. The method of the present invention provides security that prevents tampering and false evidence of postage payment and provides the ability to do batch processing of digital tokens);

receiving a request to evidence postage from a user of said plurality of users, (col. 3, lines 29-32, performing a requested vault function when an entered user password under which the request is made has been assigned vault functional access for the requested vault function, where col. 4, lines 19-22 shows the present invention is applicable to any-value metering system that includes a transaction evidencing.);

(a) determining, based on the requesting user's postage usage parameter, if sufficient postage is available to fulfill the request for the requesting user (col. 7, lines 27-46, shows PC-based postage meter 10 can function as a multiple-user device in which multiple users can have different access privilege levels to the meter features and functions. In the preferred embodiment, a setup routine will allow the primary or administrative user of PC-based postage meter 10 to customize individual user passwords for access to the different meter features and functions, and shows an example where performance of the meter refill function may be restricted to the owner of the meter or a user assigned as an administrative user. This restriction is a common security feature since refilling the meter is spending money. The meter owner may also limit the number of users that are authorized to perform other functions of the meter, for example, changing any of the meter parameters, such as postage limit. Such users may

share a single password to perform certain level(s) of functions or may each be given an individual password for added security, where examiner interprets the password as the user parameter, where sufficient postage determination is inherent with evidencing of postage);

(b) determining based on at least one of said postage meter's meter parameters if sufficient postage is available from an available postage balance of said postage meter used for evidencing postage to fulfill the request for the requesting user (col. 7, lines 27-46, shows PC-based postage meter 10 can function as a multiple-user device in which multiple users can have different access privilege levels to the meter features and functions. In the preferred embodiment, a setup routine will allow the primary or administrative user of PC-based postage meter 10 to customize individual user passwords for access to the different meter features and functions, and shows an example where performance of the meter refill function may be restricted to the owner of the meter or a user assigned as an administrative user. This restriction is a common security feature since refilling the meter is spending money. The meter owner may also limit the number of users that are authorized to perform other functions of the meter, for example, changing any of the meter parameters, such as postage limit. Such users may share a single password to perform certain level(s) of functions or may each be given an individual password for added security, where examiner interprets the postage limit as the meter parameter, where sufficient postage determination is inherent with evidencing of postage);

evidencing a requested postage amount if said (a) determining is affirmative and if said (b) determining is affirmative *(*col. 7, line 64-col. 8, line 2, At step 120, a check is made to determine if the entered user password is authorized to perform such request. If not, the vault returns to an idle status at step 104, preferably sending a message to the user that the request is not authorized. If authorized, at steps 122-128, the requested function is performed,*);*

It would have been obvious to provide a database that stores a postage usage user parameter for each user of a plurality of users with the motivation of showing some type of memory associated with the vault that will store user related parameters.

Lee et al does not specifically disclose the following, however, Liechti discloses:

recording postage usage for the requesting user in the postage usage database (Liechti: col. 7, lines 4-6; col. 12, lines 22-24); and

deducting an amount of postage used to fulfill the request for the requesting user from the available postage balance (Liechti: col. 7, lines 4-7).

It would have been obvious to disclose the above limitations with the motivation of showing the final steps of evidencing a postage meter.

As per claim 30, Lee et al discloses:

authenticating the requesting user (col. 8, lines 17-18, the term password is used generically and refers to present and future methods for authenticating users and col. 7, line 64-col. 8, line 2, At step 120, a check is made to determine if the entered user password is authorized to perform such request)

As per claim 31, Lee et al discloses:

receiving a request to configure parameters for the requesting user (col. 3, lines 5-20, Each of the modes is assigned with a user password that is required to operate the vault in the respective mode. Each user of the vault is provided with one or more passwords corresponding to the access level assigned to the user); and

modifying at least one of the user parameters in the postage usage database, (col. 2, lines 50-65, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password).

As per claim 32, Lee et al discloses:

the usage limit is a maximum amount of postage that can be evidenced for the requesting user (Col. 2, line 61, maximum postage amount).

As per claim 33, Lee et al discloses:

receiving a request to purchase postage for the requesting user (col. 4, lines 11-14, PC meter system 10 includes a conventional personal computer configured to operate as a host to a removable metering device or electronic vault, generally referred to as 20, in which postage funds are stored, where the Examiner interprets storing funds on the user's account to imply receiving a request to purchase postage.); and

adding a purchased postage value to the user parameter database for the requesting user (col. 2, lines 50-65, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password).

As per claim 36, Lee et al discloses:

wherein the at least one parameter comprises at least one of time and amount (Col. 2, line 61, maximum postage amount).

As per claim 37, Lee et al discloses:

wherein the particular user is associated with at least two user parameters (col. 2, lines 41-45, The method provides password controlled access to the PC-based metering system wherein the use associated with each user password can be customized for restricted access to various functions of the metering system, and col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open metering system in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password. Examples of such user functions/features that are customized to a user password are: vault refill, network meter access, maximum postage amount,)

As per claim 40, Lee et al does not specifically disclose wherein said at least one meter postage usage parameter is a meter balance, however, Liechti et al in col. 10, lines 18-45 shows meter balance is incorporated into the meter parameter. It would have been obvious to combine the teachings of Lee et al and Liechti et al to disclose wherein said at least one meter postage usage parameter is a meter balance with the motivation of showing that meter balance can be incorporated into evidencing of postage.

As per claim 41, Lee et al discloses:

a postage evidencing meter, (col. 3, line 31, shows PC-based postage meter);
a postage information system communicatively coupled to said postage evidencing meter, (col, 3, lines 41-47, PC meter system 10 may also include an optional modem 29 which is located preferably in PC 12. Modem 29 may be used for communicating with a Postal Service or a postal authenticating vendor for recharging funds (debit or credit). In an alternate embodiment the modem may be located in PCMCIA card 30);

wherein the postage information system includes a database for separately storing at least one postage usage user parameter for a user of a plurality of users of said postage evidencing meter, wherein a particular user parameter associated with a particular user establishes usage thresholds which limit an ability of the particular user to evidence postage using the meter, and wherein each respective particular user is associated with a particular respective user parameter, ((col. 8, lines 41-46, users may share a single password to perform certain level(s) of functions or may each be given an individual password for added security. PC-based postage meter 10 keeps a log, which is stored on hard drive 24, of all transactions and logins for further security, w/ lines 38-47, shows that the Electronic vault 20, is housed in a removable card, such as PCMCIA card 30, thereby making it obvious to have a database that stores a postage usage user parameter for each user of a plurality of users, col. 7, lines 27-46, shows PC-based postage meter 10 can function as a multiple-user device in which multiple users can have different access privilege levels to the meter features and functions. In the preferred embodiment, a setup routine will allow the primary or administrative user

of PC-based postage meter 10 to customize individual user passwords for access to the different meter features and functions, and shows an example where performance of the meter refill function may be restricted to the owner of the meter or a user assigned as an administrative user. This restriction is a common security feature since refilling the meter is spending money. The meter owner may also limit the number of users that are authorized to perform other functions of the meter, for example, changing any of the meter parameters, such as postage limit. Such users may share a single password to perform certain level(s) of functions or may each be given an individual password for added security);

wherein the meter parameter establishes usage thresholds for all users of said plurality of users, (col. 2, lines 41-45, The method provides password controlled access to the PC-based metering system wherein the use associated with each user password can be customized for restricted access to various functions of the metering system, and col. 2, lines 50-65, The present invention provides security management of multiple users with different privileges that access the different functionality's of the PC-based open metering system in user mode. For example, once activated the user password system requires a valid user password to be entered before the vault can be accessed. Once a user password is entered, the features or functions of the metering system available to the user depends on what functions/features were customized as being accessible for the entered user password. Examples of such user functions/features

that are customized to a user password are: vault refill, network meter access, maximum postage amount,);

wherein said postage evidencing meter is operable to access said database through a communication module to limit the ability of said particular user of said plurality of users to evidence postage in accordance with the at least one associated particular user parameter and the at least one meter parameter, (col. 7, lines 27-46, shows PC-based postage meter 10 can function as a multiple-user device in which multiple users can have different access privilege levels to the meter features and functions. In the preferred embodiment, a setup routine will allow the primary or administrative user of PC-based postage meter 10 to customize individual user passwords for access to the different meter features and functions, and shows an example where performance of the meter refill function may be restricted to the owner of the meter or a user assigned as an administrative user. This restriction is a common security feature since refilling the meter is spending money. The meter owner may also limit the number of users that are authorized to perform other functions of the meter, for example, changing any of the meter parameters, such as postage limit. Such users may share a single password to perform certain level(s) of functions or may each be given an individual password for added security).

It would have been obvious to provide a database that stores a postage usage user parameter for each user of a plurality of users with the motivation of showing some type of memory associated with the vault that will store user related parameters.

Lee et al does not specifically disclose wherein the database also includes at least one postage usage meter parameter, however, Liechti et al in col. 10, lines 18-45 shows meter balance is incorporated into the meter parameter. It would have been obvious to combine the teachings of Lee et al and Liechti et al to disclose wherein said at least one meter postage usage parameter is a meter balance with the motivation of showing that meter balance can be incorporated into evidencing of postage.

As per claim 42, Lee et al does not specifically disclose wherein said at least one meter postage usage parameter is a meter balance, however, Liechti et al in col. 10, lines 18-45 shows meter balance is incorporated into the meter parameter. It would have been obvious to combine the teachings of Lee et al and Liechti et al to disclose wherein said at least one meter postage usage parameter is a meter balance with the motivation of showing that meter balance can be incorporated into evidencing of postage.

12. Claims 12, 13,19, 20, 22, are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee et al and further in view of Manduley, U.S. Publication No. 2004/0098354.

As per claim 12, Lee et al does not teach the communication link is a wireless link.

Manduley teaches the communication link is a wireless link (Manduley: paragraph 0039). It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the system of Lee et al to have included the communication link is a wireless link as taught by Manduley for the advantage of providing a convenient way for postage meters to communicate with one another.

As per claim 13, Lee et al fails to disclose wherein the communications link is a wireline link, however, Manduley teaches in [0039] that the connection between two postal meters 100.sub.a and 100.sub.b, as shown in FIGS. 3a and 3b, can be wired or wireless.

It would have been prima facie obvious to one of ordinary skill in the art at the time the invention was made to have modified the system of Lee et al and further in view of Manduley to have included as taught by Manduley for the advantage of providing a convenient way for postage meters to communicate with one another.

As per claim 19, Lee et al does not teach the communication link is a wireless link. Manduley further teaches the communication link is a wireless link (Manduley: paragraph 0039).

It would have been prima facie obvious to one of ordinary skill in the art at the time the invention was made to have modified the system of Lee et al and further in view of Manduley to have included the communication link is a wireless link as taught by Manduley for the advantage of providing a convenient way for postage meters to communicate with one another.

As per claim 20, Lee et al fails to disclose wherein the communications link is a wireline link, however, Manduley teaches in [0039] that the connection between two postal meters 100.sub.a and 100.sub.b, as shown in FIGS. 3a and 3b, can be wired or wireless.

It would have been prima facie obvious to one of ordinary skill in the art at the time the invention was made to have modified the system of Lee et al and further in view of Manduley to have included as taught by Manduley for the advantage of providing a convenient way for postage meters to communicate with one another.

As per claim 22, Lee et al does not teach an exchange between two meters is bi-directional.

Manduley further teaches an exchange between two meters is bi-directional (Manduley: paragraphs 0034-0037 - The Examiner notes, one meter can send funds to another meter and vice versa.). It would have been prima facie obvious to one of ordinary skill in the art at the time the invention was made to have modified the system of Lee et al and further in view of Manduley to have included an exchange between two meters is bi-directional as taught by Manduley for the advantage of effectively transmitting and updating data between meters without the need for connecting to a remote data center.

Response to Arguments

13. Applicant's arguments with respect to claims 2-7, 9-13, 15-22 and 29-42 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Akiba K Robinson-Boyce whose telephone number is 571-272-6734. The examiner can normally be reached on Monday-Friday 9am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Hayes can be reached on 571-272-6708. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the •Patent Application Information Retrieval (PAIR) system, Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

A. R. B.
May 21, 2010

/Akiba K Robinson-Boyce/
Primary Examiner, Art Unit 3628